RECEIVED
CENTRAL FAX CENTER
APR 12 2006

ZILKA·KOTAB
PC
ZILKA, KOTAB & FEECE™

100 PARK CENTER PLAZA, SUITE 300
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573
FAX (408) 971-4660

FAX COVER SHEET

Date:	April 12, 2006	**Phone Number**	**Fax Number**
To:	Examiner Homayounmehr		(571) 273-8300
From:	Kevin J. Zilka		

Docket No.: NAI1P317/01.185.01 **Application No.: 10/091,645**

Total Number of Pages Being Transmitted, Including Cover Sheet: 29

Message:

Please deliver to Examiner Homayounmehr.

Thank you,

Kevin J. Zilka

☐ *Original to follow Via Regular Mail* X *Original will Not be Sent* ☐ *Original will follow Via Overnight Courier*

****
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.
****

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER
ANY OTHER DIFFICULTY, PLEASE PHONE Erica
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

April 12, 2006

RECEIVED
CENTRAL FAX CENTER

APR 12 2006

Practitioner's Docket No. NAI1P317 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Handog Wu et al.

Application No.: 10/091,645 Group No.: 2132
Filed: 03/05/2002 Examiner: Homayounmehr, F
For: NETWORK INTRUSION DETECTION AND ANALYSIS SYSTEM AND METHOD

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on January 12, 2006.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
(When using Express Mail, the Express Mail label number is mandatory; Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

_ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
_ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ (mandatory)

TRANSMISSION

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.

Date: 4/12/2006

Signature

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

PAGE 2/29 * RCVD AT 4/12/2006 7:25:14 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/7 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):06-22

04/13/2006 SFELEKE1 00000076 501351 10091645
01 FC:1251 120.00 DA

RECEIVED
CENTRAL FAX CENTER

APR 12 2006

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	$500.00
Appeal Brief fee due	**$500.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for one month:

Fee: $120.00

If an additional extension of time is required, please consider this a petition therefor.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$500.00
Extension fee (if any)	$120.00
TOTAL FEE DUE	**$620.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of $620.00 to Deposit Account No. 50-1351.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P317).

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PAGE 3/29 * RCVD AT 4/12/2006 7:25:14 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/7 * DNIS:2738300 * CSID:4089714660 * DURATION (mm-ss):06-22

RECEIVED
CENTRAL FAX CENTER
APR 12 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Handong Wu et al.	Group Art Unit: 2132
Application No. 10/091,645	Examiner: Homayounmehr, Farid
Filed: 03/05/2002	Date: April 12, 2006
For: NETWORK INTRUSION DETECTION AND ANALYSIS SYSTEM AND METHOD	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 01/12/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST
II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI ISSUES
VII ARGUMENTS

VIII APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY APPELLANT IN THE APPEAL

X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, below is a list of such appeals, interferences, or related judicial proceedings.

No such pending appeals, interferences, or related judicial proceedings exist.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-8, 10-11, 14-16, and 18-22

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1-8, 10-11, 14-16, and 18-22
3. Claims allowed: None
4. Claims rejected: 1-8, 10-11, 14-16, and 18-22
5. Claims cancelled: 9, 12, 13, 17

C. CLAIMS ON APPEAL

The claims on appeal are: 1-8, 10-11, 14-16, and 18-22

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there is no amendment after final.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claims 1 and 19, as shown in Figures 1-5, a system, method, and computer program product are included for providing an intrusion detection and analysis system. Included is a data monitoring device (e.g. see item 16 of Figure 1, etc.) comprising a capture engine (e.g. see item 32 of Figure 3, etc.) operable to capture data passing through the network in response to a trigger and configured to monitor network traffic. Also, the data monitoring device involves decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups. Finally, the data monitoring device analyzes received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors. An intrusion detection device (e.g. see item 14 of Figure 1, etc.) is separate from the data monitoring device. The intrusion detection device includes a detection engine (e.g. see item 34 of Figure 3, etc.) operable to perform intrusion detection on data provided by the data monitoring device. Further, the intrusion detection device includes application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection. Finally, the intrusion detection device includes memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred. In use, the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device. For example, the intrusion detection device is allowed to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device. Also, the intrusion detection device is allowed to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device. See, for example, page 7, line 3 – page 12, line 17 et al.

With respect to a summary of Claim 11, the above summary of Claims 1 and 19 is incorporated by reference, at least in part. As shown in Figure 4, the intrusion detection device is coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device. Specifically, an associated method comprises receiving data at the data monitoring device. In addition, the method comprises capturing at least a portion of the packets contained within the data (e.g. see item 62 of Figure 4, etc.). Still yet, the method comprises

allowing the intrusion detection device to call at least one application program interface configured to open applications of the data monitoring device. Even still, the method comprises performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device (e.g. see item 66 of Figure 4, etc.). See, for example, page 7, line 3 – page 13, line 17 et al.

VI ISSUES (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 21 and 22 under 35 U.S.C. 112, first paragraph, as not being enabled.

Issue # 2: The Examiner has rejected Claims 21 and 22 under 35 U.S.C. 112, second paragraph, as failing to define the invention.

Issue # 3: The Examiner has rejected Claims 1-19 under 35 U.S.C. 102(e) as being anticipated by or, in the alternative, unpatentable under 35 U.S.C. 103(a) as being obvious over Vaidya (U.S. Patent No. 6,279,113) in view of Porras (U.S. Patent Application No. 2003/0101358).

VII ARGUMENTS (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 21 and 22 under 35 U.S.C. 112, first paragraph, as not being enabled. With respect to Claim 21, the Examiner has questioned the exact implication of the "frame_context_pointer_position" limitations. With respect to Claim 22, the Examiner has stated that Page 12 of the specification only mentions the incision of "frame_tcp_bridge," "frame_udp_bridge," "frame_ip_bridge," and "frame_http_bridge," but does not give a description of the specific functionality of such elements.

Appellant respectfully asserts that Page 12 of appellant's disclosure describes the form the API's may take, or, in other words, defines the form that the API takes. Thus, according to the claims, the API is defined according to "frame_context_pointer_position" (Claim 21) which includes "frame_tcp_bridge; frame_udp_bridge; frame_ip_bridge; and frame_http_bridge" (Claim 22).

Issue # 2:

The Examiner has rejected Claims 21 and 22 under 35 U.S.C. 112, second paragraph, as failing to define the invention. Appellant respectfully disagrees. In particular, the Examiner has simply made a blanket assertion regarding this issue without providing any specifics. To this end, appellant respectfully finds the Examiner's rejection baseless.

Issue # 3:

The Examiner has rejected Claims 1-20 under 35 U.S.C. 102(e) as being anticipated by or, in the alternative, unpatentable under 35 U.S.C. 103(a) as being obvious over Vaidya (U.S. Patent No. 6,279,113) in view of Porras (U.S. Patent Application No. 2003/0101358).

Group #1: Claims 1-8, 10, 14-15, and 18-20

With respect to each of the independent claims, and specifically appellant's claimed "intrusion detection device separate from the data monitoring device," the Examiner has argued, in the latest Office Action dated 11/30/2005, that appellant's claimed "intrusion detection device separate from the data monitoring device" is only separate in functionality. Appellant respectfully points out page 7, line 14-page 8, line 6, along with associated Figure 1, which clearly shows that the network analysis and data monitoring device 16 and the intrusion detection device 14 are separate devices, and not merely that they perform separate functionality, as the Examiner contends.

The Examiner has also argued that Vaidya does not limit his invention to one processor only. In making such an assertion, the Examiner has referenced Figure 4, items 36, 34 and 38 as being separate modules to perform separate functionalities. Appellant respectfully asserts that Figure 4 only discloses modules that work with the virtual processor, but not that such modules are separate processors. Thus, appellant respectfully asserts that the only processing device in Vaidya is the virtual processor. Furthermore, the modules relied on by the Examiner do not provide the separate functionality claimed by appellant, namely "captur[ing] data passing through the network," "perform[ing] intrusion detection," etc.

Still yet, the Examiner has argued that Vaidya performs the functionality of appellant's data monitoring device and intrusion detection device in item 36, but that such functionality is separate as shown in item 40. Appellant respectfully asserts that item 40, the register cache, "temporarily stores information extracted from a data packet which determines which signature profile(s) will be accessed from the signature profile memory 39." Clearly, such register cache that only extracts information from data packets does not meet appellant's claimed "data monitoring device," which specifically "capture[s] data passing through the network," "monitor[s] network traffic," "decode[s] protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups," and "analyze[s] received data," in the manner claimed by appellant. Thus, the functionality of items 36 and 40, as relied on by the Examiner, does not meet appellant's specific claim language.

Furthermore, the Examiner has argued that Vaidya's claim 1, which claims a method of detecting intrusion attempts, is broken down into several steps, including monitoring network traffic and network intrusion. Appellant emphasizes that merely claiming separate steps does not meet appellant's separate devices, as claimed. In addition, simply claiming monitoring network traffic, as in Vaidya, does not meet appellant's specifically claimed functionality of a data monitoring device that exceeds beyond monitoring network traffic, as excerpted above.

Appellant again respectfully asserts that the appellant's arguments made in the Office Action dated 10/12/2005 on page 7, paragraph 4-page 9, paragraph 1 clearly show the distinction between Vaidya and appellant's specific claim language.

With respect to appellant's claimed technique "wherein the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device," the Examiner has argued that such claim language in addition to the specification does not point out any advantage in separation of the intrusion detection device and the data monitoring device. In response, appellant points out page 8, lines 3-6 which states that the components, including the intrusion detection device and the network analysis and data monitoring device can perform dual simultaneous functions, etc. which allows for efficient detection of intrusions in high-speed network traffic.

The Examiner has also argued that such aforementioned claim language would have been obvious and well known to a person skilled in the art, and noted Porrass in such regard. Specifically, the Examiner has argued that the motivation to use APIs in order to build the intrusion detection system would have been to take advantage of an already prepared and well tested element to perform part of the required functionality. Appellant respectfully asserts that the alleged obviousness of utilizing APIs does not make appellant's specific claim language obvious, since appellant does not merely claim using APIs, but instead specifically claims "allowing the intrusion detection device to call an application program interface configured to

open a protocol decoding application associated with the separate data monitoring device, and...allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device." Thus, each device, as claimed by appellant, is allowed to call API's with specific separate functionality such that the intrusion detection device is allowed to leverage the separate data monitoring device. These claimed features are simply non-existent in both Vaidya and Porrass.

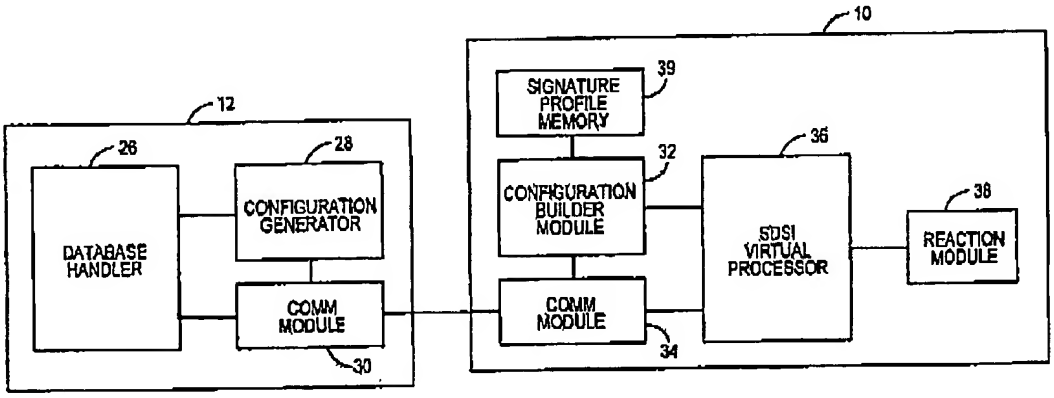
With respect to the 102 rejection, the Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

With respect to the 103 rejection, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references fail to teach or suggest all of the claim limitations, as noted above.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Group #2: Claim 11

With respect to independent Claim 11, appellant incorporates the arguments made hereinabove regarding Group #1. Further, it is noted that Claim 11 includes additional language requiring a technique of "... allowing the intrusion detection device to call at least one application program interface configured to open applications of the data monitoring device; and performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device" (emphasis added). The Examiner relied upon items 26, 32, 34, 36, and 39 of Fig. 2, and Col. 6, lines 1-11 (see below) from Vaidya to make a prior art showing of such claim language.



(Vaidya, Fig. 2)

"Each data collector 10 includes a communication module 34 for transmitting and receiving information to and from the data repository 12. A configuration builder module 32 assigns a set of signature profiles to each network object and stores data representative of associations between network objects and attack signature profile sets in a signature profile memory 39. The configuration builder module 32 accesses the appropriate attack signature profile sets during operation of the data collector 10 and provides the attack signature profiles to a stateful dynamic signature inspection (SDSI) virtual processor 36. The attack signature profiles include a set of instructions which the virtual processor 36 executes to determine whether a particular data packet is associated with a network intrusion. Although a preferred embodiment of the processor employs the software based virtual processor 36 to execute attack signature profiles, a hardware based processor can be employed in the place of the virtual processor 36." (Vaidya, Col. 6, lines 1-11 - emphasis added)

The Examiner has further argued that "the configuration builder module (item 32) allows the intrusion detection device (item 36) access attack signature profiles stored in signature profile

memory (item 39)." However, the excerpts merely suggest a technique where "[t]he configuration builder module 32 accesses the appropriate attack signature profile sets during operation of the data collector 10 and provides the attack signature profiles to a stateful dynamic signature inspection (SDSI) virtual processor 36" (emphasis added). Further, the Examiner has argued that "the communication module (item 34) allows intrusion detection device access the data in database handler (item 26)." Again, appellant respectfully asserts that the excerpt simply teaches a technique where"[e]ach data collector 10 includes a communication module 34 for transmitting and receiving information to and from the data repository 12" (emphasis added).

To this end, there is clearly not even a suggestion in the above excerpts of a technique of "allowing the intrusion detection device to call at least one application program interface configured to open applications of the data monitoring device; and performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device" (emphasis added), as claimed by appellant.

Group #3: Claim 16

With respect to dependent Claim 16, the Examiner has relied on the following excerpts from the Vaidya reference to make a prior art showing of appellant's claimed technique "wherein the application program interfaces provide parsing of signatures used in signature matching" (see Claim 16).

> "The sequential signature attribute refers to multiple expressions which are sequentially executed on successively transmitted data packets associated with an application session. If each of the expressions detects the event it was designed to detect, a network intrusion has been detected.
>
> A more formal description of an attack signature in a loose BNR parsing grammar follows:
>
> ```
> Pattern        := Hex or ASCII string of characters
> Offset         := integer
> Protocol       := one of the communication protocols, ie. MAC-layer
>                  Network-layer, Transport-layer, or Application-layer
> Extract_Type:= Byte, Word, Long Word or String
> Header_Field:= Predefined keywords for communication
>                  protocol header fields
> Variable_Name:= ASCII character string Name
> SP             :=<Pattern, Offset, Protocol> . . . Search Primitive
> VP             :=<Extract_Type, Offset, Protocol> . . . Value Primitive
> ```

```
OP              :=<Logical> .|. <Arithmetic> .|. <Bit-wide>
                | <Association> | ... Operators
Basic_Expression:= <SP>.|.<OP>.|.<Header_Field.|.<SP OP SP>.
                |. <SP OP VP .|. <SP OP Header_Field>
Assignment := <Variable_Name> "=" <Basic_Expression>
Complex_Expression := {(<Basic_Expression> OP <Basic
                Expression>) . . . }
Expression      := <Complex_Expression> .|. <Complex_Expression>";"
                {(<Assignment>";") . . . }
Signature_Attributes := <Simple> .|. <Counter-Timer-Based>.|.
                <Sequential-occurrence>
Attack_Signature := <Signature_Attribute> { <Expression> . . . .}"
```

(Vaidya, Col. 10, lines 17-45 - emphasis added)

Appellant respectfully asserts that the excerpt above simply does not meet all of appellant's claim limitations. Specifically, the Vaidya excerpt teaches "...attack signature in a loose BNR parsing grammar..." and that the "...sequential signature attribute refers to multiple expressions which are sequentially executed on successively transmitted data packets..." The BNR parsing grammar and multiple expressions, as described by Vaidya, clearly do not, however, meet appellant's specific claim language, since Vaidya fails to even suggest a technique "wherein the application program interfaces provide parsing of signatures used in signature matching" (emphasis added), as claimed by appellant.

VIII APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) An intrusion detection and analysis system comprising:

a data monitoring device comprising a capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors;

an intrusion detection device separate from the data monitoring device, the intrusion detection device comprising a detection engine operable to perform intrusion detection on data provided by the data monitoring device;

application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection; and

memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred;

wherein the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device.

2. (Original) The system of claim 1 wherein the reference network information comprises a signature database including signature profiles associated with a known network security violation and wherein the detection engine is operable to compare the data provided by the data monitoring device with the signature profiles to detect network intrusions.

3. (Original) The system of claim 2 further comprising a parser operable to parse, generate, and load signatures at the detection engine.

4. (Original) The system of claim 1 wherein the reference network information comprises a baseline state of network traffic and wherein the detect engine is operable to compare the data received by the capture engine to the baseline network state and look for anomalies.

5. (Original) The system of claim 4 wherein the data monitoring device provides the baseline state of network traffic.

6. (Original) The system of claim 1 further comprising a log file configured to at least temporarily store reports generated by the detect engine.

7. (Original) The system of claim 6 further comprising an alarm manager operable to generate alarms based on information generated by the log file.

8. (Original) The system of claim 1 further comprising a filter configured to filter out packets received at the data monitoring device.

9. (Cancelled)

10. (Original) The system of claim 1 wherein the capture engine is configured to forward packets and temporarily store packets for later analysis by the data monitoring device.

11. (Previously Presented) A method for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device including a capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors, and an intrusion detection device separate from the data monitoring device, the intrusion detection device coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device; the method comprising:

receiving data at the data monitoring device;

capturing at least a portion of the packets contained within the data;

by allowing the intrusion detection device to call at least one application program interface configured to open applications of the data monitoring device; and

performing intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device;

wherein the at least one application program interface allows the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device.

12. (Cancelled)

13. (Cancelled)

14. (Original) The method of claim 11 further comprising filtering the data prior to capturing packets.

15. (Original) The method of claim 11 wherein performing intrusion detection comprises performing signature matching.

16. (Original) The method of claim 15 wherein the application program interfaces provide parsing of signatures used in signature matching.

17. (Cancelled)

18. (Original) The method of claim 11 wherein performing intrusion detection comprises detecting anomalies in the received data.

19. (Previously Presented) A computer program product for performing intrusion detection with an intrusion detection and analysis system comprising a data monitoring device including a

capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors, and an intrusion detection device separate from the data monitoring device, the intrusion detection device coupled to the data monitoring device and configured to perform intrusion detection on data provided by the data monitoring device; the product comprising:

code that receives data at the data monitoring device;

code that captures at least a portion of the packets contained within the data;

code that calls at least one application program interface configured to open applications of the data monitoring device;

code that performs intrusion detection at the intrusion detection device utilizing at least one of the applications of the data monitoring device; and

a computer-readable storage medium for storing the codes;

wherein the at least one application program interface allows the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device.

20. (Previously Presented) The computer program product of claim 19 wherein the computer readable storage medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive.

21. (Previously Presented) The system of claim 1 wherein at least one of the application program interfaces take the form of frame_context_pointer_position.

22. (Previously Presented) The system of claim 1 wherein at least one of the application program interfaces include:
frame_tcp_bridge,

frame_udp_bridge,
frame_ip_bridge, and
frame_http_bridge.

IX APPENDIX LISTING ANY EVIDENCE RELIED ON BY APPELLANT IN THE APPEAL (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P317).

Respectfully submitted,

By: _____ Date: 4/12/06

Kevin J. Zilka

Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660